A SYSTEM AND METHOD FOR MANAGING RISKS ASSOCIATED WITH OUTSIDE SERVICE PROVIDERS

CROSS REFERENCE TO RELATED APPLICATIONS

[01] This application claims priority to United States Provisional Application number 60/411,284, filed on September 17, 2002 the entirety of which is incorporated herein by reference.

FIELD OF THE INVENTION

[02] The present invention generally relates to systems and methods for managing risk, and more particularly to systems and methods for managing the risk associated with outside service providers.

BACKGROUND OF THE INVENTION

[03] Risk management relates to procedures for assessing and managing risk that are established by the enterprise, with accompanying directives by management to comply with the procedures. For example, a given manager of a department may be required to establish the level of risk associated with the operation of a particular computer system (e.g., the risk of losing use of such a computer system for some period of time). This manager may formulate a system for evaluating and reporting the risk, that can be used by lower level and project managers. For example, on a periodic basis such as quarterly, the managers for a given department might be required to communicate to upper management the various risk factors and risk evaluations that are related to its computer information systems operations. The risk factor related information can be documented through various forms or questionnaires for evaluating risk and risk factors associated with projects for which they are

responsible. These forms and questionnaires can be compiled into reports and other summary data to provide a department manager with a fairly good idea of the level of compliance with various enterprise procedures.

[04] Typically, if a group within the department is not in compliance with the established procedures for the enterprise, this information can be so noted in the summary or compiled data presented to the department manager. In such a case, the department manager can establish plans to bring the group into compliance, and to monitor the status of the group in progressing with the plan.

[05] The impact of evaluating the risk for a given enterprise can have serious consequences with regard to the success or profitability of the enterprise. For example, if an enterprise fails to adequately assess the impact of the loss of a particular facility for some period of time, such a loss can catastrophic to the business. In addition, if the enterprise has established procedures that are designed to protect the enterprise from liability, or otherwise assure that levels of risk within the enterprise are minimized, the enterprise can be exposed to tremendous liability if the procedures are not properly followed. For example if the enterprise has contractual obligations that could only be met through the use of a particular facility.

[06] In typical enterprises, the analysis, statuses and reporting to upper management of the procedures with respect to crisis management and business recovery are often haphazard, and inconsistent. For example, some managers may find the requirement of filling out forms and answering questionnaires to be an inefficient use of time, and fail to effectively complete risk assessments. Other managers may take the attitude that 'it can't happen here'. Furthermore, most departments fail to evaluate the external dependencies that it has, and the impact on its ability to perform its functions should those external entities experience a catastrophic event.

[07] One of the significant risks corporations face that is associated with external dependencies is the reliance on Outside Service Providers (OSP). As more and more corporations are outsourcing part of their operations, the reliance on such OSPs is growing. One of the more prevalent areas of such outsourcing is in the area of software application development, maintenance, operation and security monitoring services. OSPs are often asked to process and store company critical and confidential data. In accessing the risk to the corporation, the impact of the failure of an OSP to provide the contracted for services must be an integral part of the corporation's risk assessment methodology.

[08] Where tools for these types of risk assessments do exist., they tend to be form intensive, and inconsistent between various enterprise locations. It is difficult to track and maintain the data that can be obtained from forms related to assessment of risk, and even more difficult to take an enterprise view of such risk, which is absolutely required for major disruptive events. Most such tools are paper based, which clearly are inadequate during an actual event and are similarly inadequate in recovering from such an event. For OSPs, the assessment task is even more complicated as the policies and procedures followed by the OSP must be assessed.

[09] Some computer based systems have been developed to overcome the difficulties with traditional paper based risk assessment systems. It does not appear that any such systems have been developed with respect to assessing and containing the risk associated with OSPs.

SUMMARY OF THE INVENTION

[10] The present invention is a system and method for assessing the risk associated with OSPs. In the preferred embodiment, an OSP is a outside organization that has been retained to process or store information for the enterprise, provide production

support or maintenance, provide security monitoring services, provide call center services, or develop applications and/or systems. OSPs are also referred to as "third party service providers" or "external service providers." Although the above list of services are those provided by OSPs in the preferred embodiment, the present invention is clearly applicable to OSPs that provide other services. The system and method of the present invention provides the capabilities to manage and monitor the various components of an onshore/offshore Information Security program. This invention enhances current processes to provide a decision engine around key issues providing the capability for enhanced, monitoring and management around the risk management capabilities of the OSP.

[11] A first step of the present invention is to create a core repository that manages, monitors and measures all OSP assessments across an institution (e.g., a corporation). The invention eliminates redundant systems and functions related to OSP assessment within each of the Lines of Business (LOBs) of the institution.

[12] The present invention utilizes a six-step OSP management system to develop, assess and test the risk associated with the OSPs employed by a corporation. The system identifies and tracks outstanding issues related to the OSP through final resolution or acceptance of the risk posed by the OSP issue. The system and method employs automated questionnaires that require responses from the user (preferably the manager of the OSP relationship). The responses are tracked in order to evaluate the progress of the assessment and the status of the OSP with respect to compliance with the enterprise's requirements for OSPs. One or more responsible parties for a given area are identified or appointed to be responsible for responding to compliance questionnaires. The parties fill in questionnaires designed to focus on various features of risk assessment for specific aspects of the operation of an OSP. For example, the responsible parties for an area that contracts for data storage by the OSP would be

asked assess the OSP preparedness in the case of a disaster (e.g., a fire). The rating for disaster recovery readiness may depend upon such factors as whether information is stored off site on a regular basis, intervals in which system backups are made, robustness of computer recovery systems and so forth.

[13] Once a questionnaire has been completed, the OSP can be given an overall rating of exposure to various forms of risk. Areas of risk can be acknowledged, prompting a sensitivity rating, such as severe, negligible and so forth. Once risk is acknowledged, a plan for reducing the risk or bringing the OSP into compliance can be formulated, and progress towards compliance can be tracked. Alternatively, an identified exposure to risk can be disclaimed through the system, which requires sign off by various higher level managers and administrators.

[14] Once risk assessment is completed for various OSPs, a higher level manager can review exposure to risk on a broad perspective, and through a user interface, expand particular areas where high risk is identified as a problem. A risk category that is expanded reveals the different departments and/or projects which use OSPs and their associated risks or compliance statuses. The higher level manager can thus identify particular projects, activity areas and/or OSPs where risk exposure exists.

[15] The sensitivity of the risk factors can also be gauged and used to develop an overall risk rating. For example, a person responsible for assessing the risk related to a particular OSP is asked to rate the sensitivity of various hypothetical events such as competitive disclosure, financial loss or impact on perception of customers.

[16] Requirements for compliance with regulatory demands and regulatory agencies are built into the OSP risk management tool. Project managers and higher level managers can determine in a glance if a particular OSP's practices and procedures are in compliance with regulatory guidelines. Higher level managers have broader access

than lower level mangers to risk assessment information according to level of seniority. For example, a middle level manager can see all the risk assessment factors for each OSP relationship that they manage, but can see no risk information beyond their allotted level. A high level manager can view all the information available to the mid level manager, in addition to any other manager or group for which the high level manager has responsibility. Accordingly, access to the system is provided on a secure basis that is reflective of the user's level of seniority.

[17] The system also provides security features such as logon IDs and passwords. Access levels are assigned based on seniority or management status, and provide a mechanism for a secure review of risk exposure and compliance. Once data is entered into the system it cannot be modified unless the user has proper authorization. The system generates reports to inform persons or groups about their compliance status. A search tool is available for locating various OSPs, business units, compliance areas, risk status levels and so forth. The system can also be used for training users on risk management policies, how risks are evaluated and how paths to compliance can be determined.

[18] The system according to the present invention thus provides immediate compliance verification, a calendar of events, allows shared best practices and corrective action plans and provides a mechanism for risk acknowledgement communicated to other members of a hierarchy. The system can be used in any hierarchical organization including such risk sensitive enterprises as military units, space missions and highly financed business endeavors.

BRIEF DESCRIPTION OF THE DRAWINGS

[19] For the purposes of illustrating the present invention, there is shown in the drawings a form which is presently preferred, it being understood however, that the invention is not limited to the precise form shown by the drawing in which:

[20] Figure 1 illustrates the system of the present invention;

[21] Figure 2 depicts a high level view of the process of the invention;

[22] Figure 3 is the interface of system 10 for describing an OSP;

[23] Figure 4 illustrates the impact assessment interface;

[24] Figure 5 illustrates the Country Impact interface;

[25] Figure 6 depicts Roles and Responsibilities interface;

[26] Figure 7 is an OSP review interface with respect to application development;

[27] Figure 8 illustrates the OSP continuity preparedness review interface;

[28] Figure 9 illustrates the contact interface;

[29] Figure 10 depicts a Privacy interface;

[30] Figure 11 illustrates a State of Health Report Card status screen;

[31] Figure 12 illustrates a legend to the icons depicted in Figures 11 and 13; and

[32] Figure 13 is a detailed State of Health Report Card status screen.

DETAILED DESCRIPTION OF THE INVENTION

[33] The system 10 of the present invention is illustrated in Fig. 1. As illustrated, system 10 is implemented using a distributed client/server architecture. The clients 15 (one illustrated) are distributed throughout the enterprise (corporation), while the servers 20 are centrally located with redundancies (not illustrated). This infrastructure consists of one application server 25 communicating with application database 35, and one database server 30 communicating with database 40. In a preferred

embodiment, the application server 25 is running BEA WebLogic 5.1 that comprises middleware between the front-end web application and the application database 35. In this preferred embodiment, database server 30 is running Oracle 8.16 Server and database 40 is an Oracle database.

[34] In the preferred embodiment, client 15 is a web based browser application. This application 15 preferably uses browsers that support Java applets and JavaScript such as Netscape 4.x or Internet Explorer 4.x. Menu applet 45 is an illustration of a Java applet supported in client 15.

[35] Figure 2 broadly describes the six step method of the present invention. The method enables tracking of OSPs across the enterprise and the six-step map provides for consistency and standardization for OSP review and risk assessment throughout the organization. The six step method further provides for a comprehensive understanding of the OSP's business resiliency components, information security alignment and privacy disciplines. The present invention matches those key elements to the needs of key business functions across the Lines of Businesses. Gaps identified by the system of the present invention in this analysis are tracked and monitored by the information security team for the enterprise using the system of the present invention.

[36] In step one (50) the person assigned with the responsibility to assess a particular OSP describes the OSP and the resources (e.g., software applications or data) accessed or supported thereby. The responsibility for describing the OSP is typically assigned to the manager in charge of the relationship with the OSP, as this is the person in the organization with the most intimate knowledge about the current state of the operation of the OSP at any given time. As further described below, the information for each OSP is aggregated and rolled up for each higher level of management with the organization. In the second half of step one (50), the user

assesses the business risk and the country impact risk associated with the particular OSP. In step two (55) of the process, various roles and responsibilities within the enterprise are defined and assigned. In step three (60) of the method, the OSP and the enterprises relationship with the OSP is reviewed with respect to the finances of the OSP, the contractual relationships with the OSP (and compliance therewith), the sourcing of the OSP contract and the controls in place in regard to external connectivity and dependencies on external systems that are not controlled by the enterprise. In step four (65) all of the security practices and mechanism of the OSP are reviewed. In step five (70) of the method, the procedures of the OSP in the event of an interruption in its business (e.g., a natural disaster) are reviewed to insure continuity of the service to the enterprise. In step five, key contacts within the enterprise as well as the within the OSP are identified. Finally, in step 6 of the process, the privacy policies of the OSP are reviewed to insure compliance with the privacy policies of the enterprise (e.g., with respect to the collection and retention of sensitive data).

[37] Figure 3 illustrates an input screen 80 employed by the user to describe the OSP. Much of the description contained herein is made in terms of the user interface screens (e.g., input screens) illustrated in the Figures. Further description herein relates to the processing of the information illustrated in these screens by the hardware components of system 10 illustrated in Fig. 1. As appreciated to those skilled in the art, the description of these screen and the accompanying description of the processing allows one to make and use system 10.

[38] Screen 80 is used to input into system 10 the descriptions of as many OSPs as are required. In field 85, the user identifies the OSP by name. A dropdown box is provided for field 85 so that the user can recall the data for a previously identified OSP and edit the information associated with that OSP is necessary (e.g., an address

change). Field 90 is used to identify the location of the OSP, preferably by Street, City, State and Zip Code. OSPs are preferably defined by one specific location. If an OSP has multiple locations, the OSP is preferably identified by the address where the OSP review was conducted. Field 95 is used to identify the specific location at which the OSP is providing services to the enterprise. Again, this location is preferably identified by Street, City, State and Zip Code.

[39] In area 100, the manager identifies the production applications of the enterprise that are supported by the OSP being reviewed. As known to those skilled in the art, a production application is an application that is actively being used by the enterprise in it's business. For each application, the user identifies the name of the application 110, the criticality of the application to the enterprise 115, the sensitivity of the application 120, and the name of the owner 125 of the information (data) associated with the application. In order to assist the user with the input of the application name, area 100 is provided with an ADD button 130. This ADD button causes a drop down list to be displayed that lists the production applications of the enterprise. In a preferred embodiment, the applications identified in the dropdown list are automatically supplied from the software application within the enterprise that performs configuration management of all of the enterprise's applications. If an OSP is no longer associated with a production application, area 100 provides a DELETE button 135 for removing the production application.

[40] The criticality 115 of the production application is determined by the business impact of the loss of the use of the application. The criticality 115 of the application is further described with respect to Fig. 4 below. The sensitivity 120 of the application is determined with respect to whether the application processes data considered to be private (e.g., Social Security numbers). In field 125, the user inputs

the person responsible for ownership of the application, typically a manager in the enterprise.

[41] In area 140, the user identifies the applications of the enterprise that are under development or under test that are supported by the OSP being reviewed. As with the production applications, for each application under development or test, the manager identifies the name of the application 150, the criticality of the application to the enterprise 155, the sensitivity of the application 160, and the name of the owner 165 of the information (data) associated with the application. Again, area 140 is provided with an ADD button 170 to assist the user in inputting the application into the system. Similarly, area 140 provides a DELETE button 175 for removing from the risk assessment system the development or test applications previously entered.

[42] As with the production applications, the criticality 155 and sensitivity 160 of the application under development or test is listed. In field 165, the user inputs the person responsible for ownership of the development application, typically a manager in the enterprise.

[43] In area 180, the user identifies whether the OSP uses a subcontractor (another vendor) to assist in the provision of services to the enterprise. The YES/NO buttons 185 are activated to indicate the answer to this question. If the OSP does use other vendors, the user is required to describe the vendor, similar to the description used for the OSP itself. As with the other areas 100 and 140, area 180 for vendors provides ADD 210 and DELETE 215 to assist the user in adding and deleting vendors in the database 40 (see Fig. 1). The manager identifies the name of the vendor in area 190. In area 195, the manager input the name of the contact at the vendor as well as other information related to the contact (e.g., phone/fax/cellular numbers). Although the information collected and analyzed with respect to the vendor is less as extensive than

the information collected about the primary OSP, the system does collect the primary location of the vendor 200 and its backup/recovery location.

[44] The primary location 200 is where the vendor primarily supplies its services. In the case that the use of the primary location is lost, area 205 identifies where the vendor would conducts its backup operations. Some vendors (and OSPs) may not have a backup location. The presence or lack of a backup location factors into the system's assessment of the risk associated vendor and/or OSP. Depending on the criticality of the services provided by the vendor and OSP, the lack of a recovery location may cause the system to determine that the risk associated with the vendor and OSP is unacceptable. Further discussion with respect to the continuity of the OSP services (e.g., primary and recovery locations) is discussed below in connection with Fig. 8.

[45] Once the manager has described the OSP to the system 10 as illustrated in Figure 3, she must then make an assessment of the relative criticality of the services provided by the OSP. Although all managers inherently believe their daily operations (i.e., supervision of the OSP relationship) are critical to the success of the organization, the system and method of the present invention attempts to take the subjectivity out this assessment to the extent practicable. System 10 does so through a series of individual assessments, from which an overall impact rating services provided by the OSP can be derived. System 10 enables corporations to assess criticality via a comprehensive information technology impact analysis. The classification focuses on loss of customer service, loss of revenue or increased operational expense, regulatory and legal penalties stemming from contractual obligations, loss of services among internal partners, and loss of competitive edge specific to visibility and industry edge. These individual impact assessments are illustrated in Figure 4. Figure 4 specifically illustrates an input screen 230 that a

manager can use to assess the impact if the OSP ceases to provide its services for some period of time.

[46] The first impact rating 235 relates to the impact of the OSP under assessment with respect to the organization's customers. Specifically, the Customer Impact Rating 235 asks the manager to assess the impact in the quality of service to existing customers of the enterprise if the OSP fails to provide its services. The assessment 235 notes that there may be intangible losses related to the degradation of service quality which will not be apparent immediately but, may create a significant financial impact in relation to the duration of the outage of the services from the OSP. List box 237 allows the user to view all of the available choices by which to answer the Customer Impact Rating 135. These possible answers include: "0" for not applicable (in the case where the OSP provides services to internal only organizations); "1" for where the manager believes there would be a 1 to 10 % decrease in the quality of service provided to the customers if the OSP's services fail; "2" for where the manager believes this degradation would be 11 to 20 %; "3" where the envisioned degradation is 11 - 30 %; "4" for a degradation of 31 - 40 %; and rating of "5" where the degradation of the impact on the customer is greater than 40 %. The specific ranges identified for responses for this field are presently preferred, and it is readily appreciated that these ranges can be modified to suit a particular business and/or objective. The Customer Impact Rating 235 relates to the quality of service to existing customers during a disaster situation. Again, there may be intangible losses related to the degradation of service quality, which will not be apparent immediately but, may create a significant financial impact in relation to the duration of the outage from the OSP.

[47] Time Frame Rating 240 asks the manager for the allowable delay of service from the OSP. The first option available for the manager to choose in list box 242 is

"More than one week'. This indicates that the services from the OSP do not have to be back up and running in any time-frame greater than the one week definition. The remainder of the impact ratings with respect to Time Frame Impact include: "1" where the OSP must resume operations within one week, (e.g., between days 3 and 7); "2" for 48 hours where it is acceptable to have OSP services resumed by the start of the business unit's second business day; "3" 24 hours , where the operations of the OSP must be resumed by the start of the business unit's next business day; "4" Intra-day, where resumption of the OSP's operations can take place before the end of the business unit's business day. (i.e. 4 to 8 hours); and "5" Immediate, where the operations of the OSP must resume within 4 hours. The specific ranges and choices identified for responses for this field are presently preferred, and it is readily appreciated that these ranges can be modified to suit a particular business and/or objective.

[48] Internal Service Agreement impact 245 relates to the responsibilities of the business unit which employs the OSP to other areas of the Corporation (e.g., as a service provider itself). For example, the department providing help desk services for internal applications would be a service provider to other departments in the organization. Some or all of the help desk functions could be outsourced to an OSP List box 147 provides the user with the range of available ratings which includes: "0" for not applicable (in the case where the department is not an internal service provider). The other acceptable choices for input into Internal Service Agreement impact 245 field are defined in terms of a time frame. The Time Frame Rating field 240 described above is a determination of how quickly the corporation needs to have available each particular business function/service. The Internal Service Agreement impact field 245 relates to the responsibilities of the department to other areas of the enterprise (e.g. as a service provider).

[49] The other available ratings for input into Internal Service Agreement impact field 245 include: "1" 1 WEEK; "2" 1 WEEK; "3" 48 HRS.; "4" 24 HRS.; and "5" INTRA DAY. The specific ranges and choices identified for responses for this field are presently preferred, and it is readily appreciated that these ranges can be modified to suit a particular business and/or objective.

[50] Financial Impact 250 relates strictly to financial losses, that would be a result of not providing business functions/services within certain time-frames. The timeframe for the calculation of the financial loss is preferably based upon a thirty (30) day outage. The selections in list box 252 include: "0" for N/A; "1" if the financial impact is estimated to be less than $500,000; "2" if the loss is between $500K and $1 million; "3" for expected losses of $1M to $2.5 M; "4" for losses of $2.5M to $5M; and "5 for estimated losses of greater than $5M. The specific ranges and choices identified for responses for this field are presently preferred, and it is readily appreciated that these ranges can be modified to suit a particular business and/or objective.

[51] Regulatory/Legal impact field 255 relates to obligations with agencies, organizations and customers that have laws, regulations or rule with which the user's business unit must comply. This includes compliance with governmental and industry regulations, contracts and service level agreements with customers, vendors, and outside agencies. List box 257 enables the user to select from several impacts that describe the legal or contractual penalties that would result from non-compliance by the department due an interruption in the business. These ratings including: "0" for N/A; "1" for a $50,000 penalty; "2" for a $50K to $100K penalty; "3" for a $100K to $500K penalty; "4" for a $500K to $1 million penalty; and "5" for a penalty of greater than one million dollars. The specific ranges and choices identified for

responses for this field are presently preferred, and it is readily appreciated that these ranges can be modified to suit a particular business and/or objective.

[52] Industry/Competitive Edge impact rating 260 relates to the effect a disaster situation would have on the particular business unit's market position and the reputation of the corporation. List box 162 gives the user the following choice for the estimated amount of impact on the market position and corporate reputation: "0" for N/A; "1" for 1 to 2 % of an impact; "2" for 3 to 5 % impact; "3" for 6 to 8 % impact; "4" for 9 to 10 % impact; and "5" for any estimated impact greater than 10 %. The specific ranges and choices identified for responses for this field are presently preferred, and it is readily appreciated that these ranges can be modified to suit a particular business and/or objective.

[53] Once the user has provided an impact assessment for each of the six categories described above (235, 240, 245, 250, 255 and 260), the user clicks on button Calculate Impact Rating 265 in order to calculate the overall impact rating of the OSP. System 10 computes criticality rating for the OSP from the number input by the manager in the categories described above. The analysis process results in a rating of 0 to 5 (low to high criticality), for each of the impact criteria. A determination of a "summary" rating is based on the highest criticality rating of the individual impact criteria. The Department Rating is: Critical (if any rating is 3, 4 or 5) or Non-Critical (if all ratings are 2 or less). The specific algorithm used to analyze the overall criticality of the department (in light of the manager's assessment) is subject to the goals of the business. For certain types of businesses, certain departments that use OSP resources will be more critical than others. For example, the restoration of the MIS department will be much more critical to a financial services business than it will be to a steel manufacturer.

[54] The above described procedure for determining the criticality of an OSP can, and is preferably performed for the vendors identified in system 10 (see Fig. 3). As previously described, the criticality of the OSP's services is cross-referenced in the OSP description screen 80, Fig. 3, in fields 115 (for OSPs) and 155 (for vendors). The criticality of the OSPs and vendors is stored in database 40 in association with the data of the particular OSP or vendor.

[55] In addition to the business impact rating for the OSP, the risk classification of step 1 (Fig. 2) also requires an assessment related to the countries in which the OSP operates. More and more, corporations are relying on OSPs that are located in countries foreign to the location of the enterprise. For example, a corporation with operations based in New York hires a software development firm in India and outsources its help desk operations to a firm in Ireland. The Country Impact Risk screen 270 asks a series of questions of the user with respect to the country in which the OSP primarily operates. In question 275, the manager is asked if there is a possibility of economic conditions and events within that country that would adversely effect the enterprise. One example of such a condition or event is a collapse of the equity markets in the country

[56] In fields 280, the user indicates whether the possibility of such conditions or events exist in the country. As shown in field 282, this determination of the user with respect to the conditions and events in the country is date stamped. It is appreciated that the conditions and events in any country are subject to daily changes, so the date of a particular determination should be tracked. If the answer to the determination is yes, there are conditions and events that would adversely impact the enterprise, the user inputs, in field 285, the source of the information on which the determination was made. For example, in field 285 as illustrated in Fig. 5, the adverse information might have come from a Government Advisory. The adverse information could also relate

to a Travel Restriction 287, news of a war 288, or from another source 290. Field 295 allows the user to input any additional and/or detailed information regarding the answer to the question. For example, the user may further describes the source of the adverse information. In area 295, the user may paste an electronic document containing the Government Advisory, or provide a link to the Advisory.

[57] Fig. 5 illustrates two more such country impact questions 300, 305, Question 300 asks if there is a possible social condition or event that would adversely impact the enterprise. An example of a social condition might be a concern is the rise of terrorism in the country that results in travel restrictions to and from the country. The user employs fields 280, 285 and 295 to supply system 10 with the requested information in regard to the question. Question 305 asks a similar question with respect to the political conditions and events. An example of a political condition might be a change in the government of the country to a more socialist administration.

[58] Based on the answers to the questions in screen 270, system 10 make determination of a rating 310 of the conditions in the country. The rating 310, either LOW or HIGH risk, is automatically computed by system 10 based upon the responses. The specific algorithm used to determine the overall risk associated with the country can be dependent on the risk tolerance of the business. The data associated with the country impact questions and the country rating are stored by system 10 in database 40 (Fig. 1). Links and cross references to the Country Impact data are additionally made the records of the OSPs and vendors conducting operations in that country.

[59] In step two of the process of the present invention (Fig. 2), the Roles and Responsibilities with respect to the operations of the OSP are identified and input into system 10 for storage in database 40 (Fig. 1). The identification of the roles and responsibilities with the corporation with respect to the operation of an OSP is a very

important exercise. Without clearly defined roles and responsibilities and specific employees of the corporation assigned these roles and responsibilities, the risks associated with the operation of the OSP can go undetected.

[60] Fig. 6 illustrates an input screen 350 for assigning personnel to the respective roles. This Figure illustrates nine different roles to be fulfilled with respect to the supervision and assessment of an OSP: Information Owner 380; Information Risk Manager (IRM) 385; Legal Manager 390; Operations Risk Manager 395; Relationship Manager for the OSP 400; Data Privacy 405; Financial Manager 410; Sourcing Manager 415; and External Connectivity Manager 420. Although nine roles are illustrated in Fig. 6 as preferred, additional roles and responsibilities can be defined and assigned using the system of the present invention..

[61] For each of the roles 355, input screen 350 indicates who performed the assignment of the role 360, when the role was assigned 365, to whom the assignment was made 370 and the date on which the assignment was accepted 375. When an assignment is made, system 10 preferably sends the assignee an email notifying the person of the assignment and the responsibilities associated therewith (see below). The assignee preferably accepts the assignment by replying affirmatively to the email and system 10 updates the applicable database to record the assignment. When a manager is making assignments in input screen 350, some of the roles will have already been pre-populated as certain of the assignments relate to firm-wide responsibilities.

[62] The following section describes the responsibilities of key ones of the roles in the present invention.

[63] The Information Owner 380 is a manager in an area which generates or processes system information (e.g., application programs and related files), or

produces products and services which depend upon system information. Each application of the enterprise must have an Information Owner 380 accountable for its protection. Applications that are cross-functional in nature, in that they serve the needs of multiple business units, preferably have a central Information Owner 380 that serves as a focal point. Local Information Owners 380 are assigned for every business unit using these applications.

[64] In each case, the Information Owner's 380 responsibilities are the most extensive and include the following relative to OSP: notifying the Information Risk Manager 385 (see below), in writing, of the intent to seek a contract with an OSP; obtaining from the OSP a copy of the OSP's latest third party financial and non-financial audit report, or internal audit report; obtaining documentation describing OSP's procedural, physical access, logical access and business recovery controls; obtaining appropriate Contract and Legal review during the development of the written OSP contract; requiring notification by the OSP of any organization, security-related, or other changes affecting the availability, confidentiality, or integrity of its services; performing an annual self-assessment to ensure continuing policy compliance; initiating the risk acknowledgment process (see below) for all instances of policy non-compliance; developing, or ensuring the development of, an essential business profile, preferably annually; ensuring the development, implementation, annual testing, and maintenance of a contingency plan (see below); assisting the Information Custodian in developing an "Operations Restoration Sequencing Plan"; Identify vital information, and direct when it shall be copied and moved to an off-premise location; certifying vital records as part of the annual contingency test; ensuring that all of the enterprise's information (e.g., application programs and related files) is evaluated through risk assessment techniques; delegating, in writing, day-to-day responsibility for protecting information kept on computer systems to the appropriate Information Custodians; authorizing each user's logical access privileges

(including application level) according to business need and maintain evidence of approval until next semi-annual review; communicating access authorizations to the technology security administration and/or business security administration of the enterprise; ensuring that access privileges of terminated/transferred users are revoked as soon as possible; ensuring that access privileges are suspended for users who are on leave-of-absence or extended disability; approving the use of specialized hardware/software which has potential to test for access control weaknesses within a business unit; reviewing access authorization to re-validate the necessity of existing user authorizations; and communicating all suspected or confirmed intrusion attempts to the IRM 385.

[65] The Information Risk Manager (IRM) 385 generally reports to senior management within the enterprise and is responsible for ensuring that the enterprise complies with the enterprises established information and technology control policies. The responsibilities of the IRM 385 includes the following relative to OSP: coordinating compliance with the requirements of the information and technology control policies; maintaining an updated list of OSP used by the enterprise and post updates to the OSP database 40; allocating resources for the OSP review process (i.e., develop appropriate OSP review team); reviewing and evaluate risk acknowledgment forms (see below), and re-evaluate existing risk acknowledgments prior to their expiration; and notifying Auditing of all approved risk acknowledgment forms.

[66] The Legal Manager 390: ensures compliance of regulatory requirements and management of regulatory risk in the region; provides awareness of regulatory requirements to all stakeholders and advice on how to achieve compliance; and reviews vendors' contractual agreement and service level agreements to ensure adequate coverage and provision for regulatory compliance globally.

[67] The Operational Risk Manager (ORM) 395 assists the executives of the enterprise in discharging their responsibilities regarding the management of operational risk.

[68] The OSP Relationship Manager 400 is an employee of the enterprise assigned by an Information Owner 380 to actively manage and monitor the OSP's performance to a service agreement between the OSP and the enterprise.

[69] Screen 350 also allows the user to assign alternates to the one or more of the roles defined as the Primary Role. In the example depicted in Fig. 6, two alternatives were assigned to fulfill primary roles, Information Owner 425 and Information Risk Manager 430. Alternative people have been identify to fulfill these two roles as they are some of the most important relative to the supervision of the relationship with OSPs.

[70] Returning to Figure 2, in step three (element 60) the manager is required to document various reviews conducted relative to the OSP. An External Connectivity Review is conducted to evaluate the controls within all architectures of the enterprise that involve a significant element of external connectivity or a dependency on external systems not controlled by the enterprise. OSPs necessarily involve external connectivity. A Financial Review is conducted in order to identify the financial stability of the OSP by evaluating the service provider's financial condition. A review of the insurance policies related to the OSP services is conducted to ensure coverage in the case of damages incurred as a result of the cessation of services.

[71] The Insurance Review includes the expiration date of the applicable policies, and the limits of liability contained therein. Some of the applicable policies include: Worker's Compensation and Employee's Liability; Commercial General Liability; Commercial Blanket Bond; and Others –such as automobile liability, motor cargo or

armored cargo. A Legal Review is conducted with respect to the contact governing the relationship with the OSP. The review of this contract includes a review of the repository of Non-Disclosure Agreements and Contracts and a review of the enterprise's records to find OSPs that have been rejected for use by the enterprise or have been terminated. A Sourcing Review is conducted to insure that the appropriate due diligence process was employed and completed in the selection of the OSP.

[72] In step four of the process (element 65, Fig. 2), a Security Review is conducted and documented. The process of the present invention provides a standardized methodology for performing on-site reviews and/or to be completed by relevant OSP personnel during the vendor evaluation process. The execution of the on-site review process entails the review of evidence (via inspection and observation) that the control procedures required by the enterprise is being performed by the OSP. Experience has shown that merely engaging in a dialogue related to the control structures that are employed at the OSP is not sufficient to ensure that the control environment is adequate. Inquiry may be sufficient to satisfy general control concerns. But inquiry alone, without inspection and observation, cannot be considered as a comprehensive on-site review. . System 10 provides a series of input screens through which the user can provide complete documentation with respect to the security review.

[73] The first series of inputs requested from the user relate to the services being provided by the OSP. The user is preferably presented with a checklist of services that the user can check off the services applicable to the particular OSP undergoing security review. The service choices preferably available for an enterprise in the financial services and banking industry include, but are not limited to: Account Verification and Closure Services; Facility Services; Anti Money Laundering; Financial Technology Services; Application Development; Fraud Management; Application Development - Production; Hardware Maintenance and Support ;

Application Development - User Acceptance Testing; Hosting; Automated Clearing House; Human Resources Management; Billing; Infrastructure Service Solutions; Business Continuity and Recovery Services; Maintenance; Call Center or Help Desk Management Services; Monitoring; Card Issuance; New Account Marketing; Cardholder Servicing; Operational Support; Change Management; Payment; Check Printer; Payroll Processing; Check Supplier; Promotion; Collection Agency; Professional Services and Support; Content Delivery Network Services; Risk Management; Customer Relationship Management; Software Maintenance and Support; Data Analysis and Reporting; Transaction Processing; Database Management; Telemarketing; Desktop Support; Vital Record Storage or Backup Processing; Electronic Banking; Voice Response Unit services; Electronic Funds Transfer; Wealth Management; Electronic Payment; Wireless Services; Electronic Presentment; Employee benefits; and Other.

[74] The questions posed to the user that is conducting the security review of the OSP are organized by topic. Fig. 7 illustrates an exemplary input screen 500, specifically questions related to application development. For each item, the user assesses the adequacy and effectiveness of the control procedures with respect to the OSP and inputs her responses. As illustrated in Fig. 7, many questions 525 have areas to provide the results of the security review in the form of Yes (505), No (510), N/A (515) answers. Additionally, screen 500 provides a Comments section 520. In the Comment section 520 the user can enter or attach a description of the control process(es) or any information, that supports or clarifies the user's responses. The user is advised to indicate what evidence exists to support the responses or cross-reference to the supporting documentation.

[75] Tables 1 through 24 illustrate preferred categories of questions and the preferred questions that are posed to the user in order to document the results of the security review of the OSP.

TABLE 1

COMPUTER OPERATIONS -- Policies and procedures should provide reasonable assurance that system capacity, availability, and operation are appropriately provided and monitored.
1. Is a process in place for monitoring system performance, including the performance monitoring tools utilized? If yes, provide the documented process and tool(s) utilized.
2. Is a process in place for monitoring network performance, including the performance monitoring tools utilized? If yes, provide the documented process and tool(s) utilized.
3. Is redundant hardware and connectivity available for all critical system functions?

TABLE 2

CONTINUITY PLANNING AND TESTING -- Policies and procedures should provide reasonable assurance that business recovery plans have been developed and tested.
1. Is there a disaster recovery plan to ensure the availability of alternative processing services should a disastrous event interrupt normal processing at the primary processing site? If Yes, please provide a copy of the contingency plan.
2. Is a back-up server/computer site facility available to provide adequate alternate processing services in the event of a disaster? If Yes, indicate name of service provider or if service provided internally and how many miles way the backup site is from the primary site.

3. Are periodic disaster recovery tests performed to validate the recovery capabilities of the critical application systems? Provide a summary of the results for the last continuity test. Provide a list of the scheduled continuity tests for next year.
4. Does the back-up processing facility have electrical power supplied via a UPS system and does it have emergency power generators to protect against local power outages?
5. Are communications links to and from the back-up recovery facility maintained and tested as part of the back-up service's on-going disaster preparedness program?
6. Is there a recovery site for the site(s) servicing JPMorgan Chase that uses a different power grid and telecommunications grid from the ones used by the primary site as required by the JPMorgan Chase Business Continuity policy and the JPMorgan Chase Business Continuity Big Rules?
7. Is there also an onshore recovery site for the site(s) servicing JPMorgan Chase as required by the JPMorgan Chase Business Continuity policy and the JPMorgan Chase Business Continuity Big Rules?
8. Will the OSP immediately notify JPMorganChase in the event of a disaster? If yes, please identify this notification process.

TABLE 3

CONTRACT MANAGEMENT -- Policies and procedures should provide reasonable assurance that service provider and subcontractor contracts contain appropriate provisions and all parties are in compliance with contract provisions.
1. Has an executed non-disclosure agreement with JPMC been documented?
2. Has a contract been signed with JPMC? If yes, provide a copy of the contract.
3. Is a service level agreement in place with JPMC? If yes, provide a copy of the SLA.

4. Has a process been established to review invoices (i.e., assure proper charges for services rendered, rate changes and new service charges)?
5. Has a process been established to review service provider/subcontractor performance relative to service level agreements, determine if contractual terms and conditions are being met and the need for revisions is evaluated?
6. Are appropriate documents and records maintained regarding contract compliance, revision and dispute resolution?
7. Does the service agreement include a clear specification of all relevant terms, conditions, responsibilities, and liabilities of both parties? Examples include: compliance, audit reporting, on-site review, notification of change/risk, SLAs, data ownership, insurance, liability, privacy, dispute resolution, problem reporting and escalation procedures, on-going monitoring, and requirements for service providers outside of the United States?
8. Have all the risk management criteria that apply to this OSP also been applied to any and all sub-contractors (of the OSP) that may have access to JPMorgan Chase data or systems?

TABLE 4

CRYPTOGRAPHY -- Policies and procedures should provide reasonable assurance that the confidentiality and integrity of critical and sensitive data is maintained.
1. Has a risk analysis been performed whether the data being transmitted has been determined to be critical and sensitive? If Yes, describe the nature of the data and level of criticality/sensitivity.

2. Is the data integrity of transaction/data protected? If Yes, describe the cryptographic mechanism used for data integrity (e.g., digital signature, what encryption algorithms are used, what is the key management process used).
3. Is the confidentiality of transaction/data protected using encryption? If Yes, describe the encryption algorithms and key management process used.
4. Is non-repudiation of transaction/data ensured using a digital signature? If Yes, describe the encryption algorithms and key management process used.
5. If JPM personal data is transmitted either to or from the third party service provider, is it encrypted in transit?
6. Is JPM personal data encrypted in storage or are appropriate access authorization models in place to ensure that the Rule of Least Privilege is being adhered to? If Yes and data is not encrypted, describe the authorization model implemented (i.e., who has access to data).

TABLE 5

DATA PRIVACY -- Policies and procedures should provide reasonable assurance that personal information transferred to an OSP is protected from unauthorized use and disclosure.
1. Does the contract require that the OSP process personal data only on our instruction?
2. Does the contract require that the OSP comply with local Data Privacy regulations?
3. Does the contract oblige the OSP to implement appropriate information security measures (i.e. treat all personal data as sensitive data)?
4. Does the contract give JPMorgan Chase the right to audit the OSP processing?
5. Does the contract provide indemnity for JPMorgan Chase in the event of a breach of contract of any of the above?

6. Is there a documented Data Privacy Policy in place and has it been reviewed by the JPMorgan Chase Data Privacy Officer?

TABLE 6

ENVIRONMENTAL CONTROLS -- Policies and procedures should provide reasonable assurance that environmental controls exist to protect these facilities.
1. Does the server/computer room have temperature and humidity control systems that are separate from the rest of the facility?
2. Are the server/computer room temperature and humidity systems actively monitored and alarmed during off-hours?
3. Do fire suppression systems and water detection systems protect the server/computer room?
4. Are fire extinguishers placed in the server/computer room?
5. Is the server/computer room electrical power supplied via a UPS (Uninterruptible Power Supply) system and are there emergency power generators? If yes, describe how long the UPS lasts, how long it takes for the generators to start-up and take over, how long the generators will run without refueling, and what steps have been taken to ensure timely refueling. Describe how often the UPS and generators tested. Indicate then the date of the last test.

TABLE 7

EXIT STRATEGY
1. Has an exit strategy been documented?

TABLE 8

FINANCIAL -- OSP's selected by JPMC should maintain a sound financial condition.
1. Has the JPMorgan Chase Information Owner evaluated a copy of the OSP's latest (i.e., not more than one year old) independent third party 'audited financial' and non-financial audit report? If applicable, provide a copy of the Annual report (if a publicly traded company) and Financial statements for the prior two years (audited if available).
2. Has a credit rating agency established a rating for the service provider (and significant subcontractors) or has some other form of financial analysis been performed? If Yes, what is the current credit rating for the service provider (and significant subcontractors)?
3. Are OSP financial obligations to subcontractors being met in a timely manner?

TABLE 9

HARDWARE CHANGE MANAGEMENT -- Do policies and procedures provide reasonable assurance that changes to the hardware configuration are authorized, tested, implemented and documented.
1. Does Information Technology (I/T) management authorize all hardware acquisitions?
2. Does the server site, network, database and application management teams coordinate the installation and testing of all hardware changes?

TABLE 10

HUMAN RESOURCES & TRAINING -- Policies and procedures should provide reasonable assurance that OSP personnel are adequately screened and trained.
1. Is the identity and background of all vendor staff servicing JPMorgan Chase known based on security background checks including drug testing and fingerprinting where permitted by law? If yes, describe the screening activities performed on job applicants (e.g., credit, drug screening, references, and criminal background checks).
2. Is there a process in place to screen the (OSP's) outside contractors such as security guards, janitorial services, etc.? If Yes, describe the process used to screen these individuals and the training process for new hires (e.g., length and breadth of training)
3. Is there an effective process by which the feedback from testing, employees' performance metrics, & quality assurance efforts are incorporated back into the training and development curriculum?
4. Is there a training program/process in place for the hiring of new employees? If yes, describe the components included in this process.
5. Is the annual rate of personnel turnover for both exempt and non-exempt workers at a level consistent with the industry?

TABLE 11

INSURANCE -- Policies and procedures should provide reasonable assurance that OSP is adequately insured.
1. Does the vendor have in place 'appropriate' insurance declaration pages? (e.g., is there sufficient insurance, underwritten by a financially sound insurer, to protect JPMorgan Chase in the event of theft (including theft of intellectual property), malicious destruction or natural disaster.) If yes, provide a copy of all appropriate insurance declaration pages.

2. Does the policy provide coverage for bonding? If Yes, how much? How much is the deductible?
3. Does the policy provide coverage for errors and omissions? If Yes, how much? How much is the deductible?
4. Does the policy provide coverage for fidelity? If Yes, how much? How much is the deductible?
5. Does the policy provide coverage for workers compensation? If Yes, how much? How much is the deductible?

TABLE 12

LOGICAL ACCESS SECURITY -- Policies and procedures should provide reasonable assurance that security administration is appropriately authorized, performed, documented and reviewed.
1. Does the vendor comply with the JPMorgan Chase requirement that two-factor authentication be used for access to JPMorgan Chase systems?
2. Is all vendor access to a JPMorgan Chase system contained so that the vendor User may only access those system resources to which he or she is authorized?
3. Are the vendor's data protection procedures sufficient to protect JPMorgan data from unauthorized access?
4. Does management authorizes access to OSP system resources (e.g., request process, logging and retention of requests, who authorizes requests, how is appropriateness of access determined)?
5. Are data access files, including access rules, regularly backed-up?
6. Are special privileges allowing security account set-up and administration limited to a segregated Security Administration function?
7. Have individuals who have access to powerful system utilities been documented? Describe how the use of these utilities are monitored.
8. Are all installation and vendor-default passwords provided with new hardware and/or system software immediately reset upon installation?

9. Is there a process to re-certify user access (e.g., how often performed, who authorizes, infrastructure versus application)? If yes, provide certification process.
10. Is there a monitoring process associated with unusual, excessive, suspicious, or unauthorized access attempts by a user, and unsuccessful log-on attempts? Is this type of activity reported to the Information Owner (OSP versus JPMC personnel)?
11. Does the access control process maintain an audit trail of User access activity?
12. Does the audit trail record, at minimum, log User sign-on and sign-off activity? If yes, describe the process used to retrieve the audit trail for investigative purposes (e.g., who performs process, how long is audit trail retained, are passwords included in audit trail)
13. Does the access control process maintain an Access Violations Log? If yes, describe the process associated with the access violation log (e.g., what type of activity is included, how long is the log retained, are passwords included, how frequently is the log reviewed, do procedures exist, how are events investigated/resolved).
14. Is Security Administration notified when OSP or JPMorganChase employees leave or change their area of responsibility?
15. Is a process in place to immediately suspend the access authorizations of Users who are terminated or transferred?
16. Are there password syntax rules in effect (e.g., password length, password complexity, password re-use)?
17. Is there a global access control options in effect (e.g., number of unsuccessful access attempts resulting in the user ID being suspended, password change interval, and workstation time-out due to inactivity, number of concurrent logins permitted)?
18. Are the passwords for super-user accounts (I.e., root – UNIX, Administrator – NT, etc.) unique to each server?
19. Is there a process in place for the setting up and utilization of administrator accounts and super-user accounts (e.g., day to day accounts versus super-user accounts, privileges assigned to accounts, uniqueness of accounts, accountability)?

20. Does a separation of duties exist between individuals who authorize access, personnel who enable access, and personnel who verify access?
21. Does a separation of duties exist between business managers who approve access and persons with Information Custodian responsibilities (other than for System Software)?
22. Does a separation of duties exist between business managers who approve access and personnel with Technology/Business Security Administration responsibilities?
23. Does a separation of duties exist between Information Owners and personnel with Technology/Business Security Administration responsibilities?
24. Does a separation of duties exist between personnel who enable access and those who review audit trails and/or violation logs?
25. Does a separation of duties exist between personnel who install and maintain the logical access control process and those who review audit trails and/or violation logs?

TABLE 13

NETWORK MONITORING AND LOG REVIEW -- Policies and procedures should provide reasonable assurance that network security event and violation logs are reviewed for all unauthorized activities in a timely manner.
1. Is a process implemented to ensure all violations and/or unauthorized activities are logged, monitored/reviewed and addressed in a timely manner by the proper level of management?
2. Are all the following security events and violations logged? • Logon and logoff failures • File and object access failures • Use of user rights failures • Restart and Shutdown -- both successes and failures • User and group management failures
3. Are full administrative privileges only allowed from the console?
4. Is protection of the vendor's network consistent with the JPMorgan Chase Network Security policy?
5. Are the vendor's security incident response procedures consistent with the JPMorgan Chase Security Incident Management policy?

TABLE 14

NETWORK TOPOLOGY -- Policies and procedures should provide reasonable assurance that the network topology is robust and secure.
1. Is a network diagram available for review that details all system connectivity? If yes, please provide a copy of the network diagram, including placement of firewalls.
2. Is the production network firewalled or physically isolated from development or User Acceptance Test networks?
3. Does the design of the network provide for alternate routing in the case of failure of the primary routing?

4. Does the network utilize diverse routing, diverse media, redundant switching facilities and multiple carriers to eliminate any single points of failure and ensure high availability?

TABLE 15

NON DOMICILE OSP -- this section gives additional evaluation criteria to be used when an OSP located overseas (outside of the US) is evaluated.
1. Has the JPMorgan Chase Legal Department, or local JPMorgan Chase counsel, determined that the local legal system is adequate, particularly in the areas of contracts, intellectual property and data privacy, to protect JPMorgan Chase? If yes, please indicate the name of the person from Legal who made this determination and provide supporting documentation.
2. Has the JPMorgan Chase country manager or Strategic Technology Sourcing determined that the country is free from political instability that would have an adverse impact on JPMorgan Chase? If yes, please indicate the name of the country manager or the person from STS who made this determination and provide supporting documentation.
3. Has the JPMorgan Chase Real Estate & Facilities Department determined that the local electrical infrastructure is adequate to protect JPMorgan Chase? If yes, please indicate the name of the country manager or the person from STS and provide supporting documentation.
4. Is the local telecommunications infrastructure adequate to protect JPMorgan Chase?

TABLE 16

OPERATIONS -- Policies and procedures should provide reasonable assurance that service provider operations are controlled effectively and reviewed by appropriate entities (internal, external, and regulatory).
1. Has a listing of internal audits performed that are related to our OSP relationship been provided (e.g. operational, technical, financial, etc.)?

2. Has a listing of external audits performed that are related to our OSP relationship been provided (e.g. SAS 70 Level II, Penetration Tests, etc.)?
3. Has a listing of Regulatory agency reviews performed that are related to our OSP relationship been provided (e.g. OCC, OTC, FTC, State, etc.)?
4. Has a copy of the External financial auditor reports been provided?
5. Has a copy of the Internal Audit Department annual review plan as it relates to our OSP relationship been provided?
6. Has a copy of due diligence reports on any sub-contractors that are related to our OSP relationship been provided?
7. Where significant deficiencies have been identified, has appropriate action plans been developed and follow-up performed?
8. Are access control reports and related monitoring reports provided to an information owner (OSP or JPMC) to identify suspicious activity.
9. Have key service provider positions been identified and appropriate succession planning performed?
10. Are periodic meetings scheduled between the service provider and the appropriate relationship manager (OSP or JPMC) to discuss performance and operational issues?
11. Is there any training that should be provided by the service provider to JPMC personnel? Are there any user groups or forums in which JPMC personnel should participate? (If no, indicate N/A.)
12. Where appropriate, is customer advocacy performance and compliance monitored by appropriate JPMC personnel?

TABLE 17

PHYSICAL SECURITY -- Policies and procedures should provide reasonable assurance that physical access to the processing environment is restricted to authorized personnel.
1. Does the company own the facility? (If leased- please document when the lease expires.)

2. Has the number of tenant occupied floors been accounted for? Describe the building tenants with common walls, floors or ceilings that are contiguous to areas occupied by the vendor.
3. Is the facility equipped with surveillance camera(s)?
4. Are the cameras monitored? If yes, provide monitoring process including hours of operation, who monitors, tape retention, etc.
5. Is there an actively monitored alarm system that physically secures the server/computer processing facility/location?
6. Is access to the facility controlled by the use of a token-based card access control system?
7. Is access to the server/computer room controlled? If yes, describe physical control process (e.g., written authorizations, type of access control system, biometrics, mantrap, re-certification of access, maintenance of access, visitor access, service technician access, business versus non-business hours).
8. Is server/computer room access and denial of access electronically logged and periodically reviewed by the security administrator?
9. Is all production server/computer equipment located in the server/computer room?
10. Do access request changes for the card access system require written approval of the site Operations Manager?
11. Are keys to cabinets, equipment rooms, and wiring closets held under proper custody? Is there a master key log?
12. Are telecommunication line junction points (wiring and router closets, etc.) secured to prevent tampering?
13. Do the OSP's policies and procedures on physical security provide reasonable assurance that physical access to the processing environment is restricted to authorized personnel?

TABLE 18

PROBLEM MANAGEMENT -- Policies and procedures should provide reasonable assurance that production problems are identified, assigned, resolved and reported in a timely manner and raised to an appropriate level in accordance with a documented process.
1. Is a process in place to address production problems (e.g., personnel involved, documentation, retention, and timeliness)?
2. Is a problem-tracking log produced that details all processing problems that occurred during the previous 24 hours? Is a unique number assigned to each problem?
3. Are changes resulting from a production problem subject to the same process as program change management?
4. Is there a documented process to track that follow-up actions are completed that will prevent a re-occurrence of production problems?

TABLE 19

PRODUCTION SUPPORT -- this section gives additional evaluation criteria to be used when an OSP is considered for production support.
1. Is the granting of emergency access to JPMorgan Chase systems consistent with JPMorgan Chase procedures?
2. Is the emergency change process consistent with the JPMorgan Chase Change Management policy?
3. Is a copy of all production source code, data, and documentation needed to install the current production system at a JPMorgan Chase facility stored at a JPMorgan Chase facility?
4. Is all elevation of system objects to production done by JPMorgan Chase personnel?
5. Is the monitoring of privileged access consistent with the JPMorgan Chase Logical Access policy?
6. Are the vendor's data protection procedures sufficient to protect JPMorgan data from unauthorized access?

TABLE 20

REMOTE ACCESS -- Policies and procedures should provide reasonable assurance that external access to the internal network is appropriately restricted, monitored and reviewed.
1. Is remote access to the internal network limited to authorized users and are their activities logged?
2. Do all users with remote access privileges require such access for their job function and has management (i.e., Information Owner) properly authorized the remote access capabilities?
3. Have any third party service providers been granted remote access privileges and is there a business requirement for such remote access?
4. Is all remote access configured to prevent war dialing? If yes, describe how this access has been configured to prevent war dialing.
5. Is there a process in place for controlling/securing devices that permit dial-in access?
6. Are clients that dial-in authenticated by the use of one-time password generation token-based technology?

TABLE 21

SYSTEMS DEVELOPMENT AND PROGRAM CHANGE MANAGEMENT -- Policies and procedures should provide reasonable assurance that new systems or changes to existing systems are properly authorized, tested, approved, implemented and documented.
1. Is there a systems development methodology / model implemented within the OSP (e.g., waterfall, prototyping, Capability Maturity Model level, etc.)?
2. Is a systems development change control process implemented (e.g., request process, documentation and retention, who approves, review/QA, testing, segregated test environments)?
3. Is each project analyzed and is a development strategy employed?
4. Does this strategy include project costing, resource requirements, and required date of implementation?

5. Is the movement of properly tested application programs into production program libraries performed by a production change control function that is independent of the development process?
6. Does the server/computer site use a source version control product to control the change management process? If Yes, what is the name of the source version control product being used
7. Is access to this source version product controlled by data access control software?
8. Is a systems software program change control process implemented (e.g., request process, documentation and retention, who approves, review/QA, testing, segregated test environments, functional versus system versus installation testing)?
9. Do the appropriate levels of management approve emergency changes, prior to implementation?
10. Are procedures in place that require that emergency changes be supported by appropriate documentation (e.g., evidence of management approval, code review)?
11. If JPMC personal data is hosted at the third party service provider, is it masked/anonymized in the development, test and/or production environments?
12. If JPMC personal data is not masked, is a procedure in place to ensure that it is deleted from the development and test environments when no longer in place?
13. Is a process implemented regarding controls over data altering utilities, user exits, privileged instructions, and libraries?

TABLE 22

VIRUS PROTECTION -- Policies and procedures should provide reasonable assurance that appropriate virus counter measures have been implemented.
1. Is a virus protection product loaded on all workstations and servers? If yes, describe what products are used with each platform within your environment.

2. Is there a process in place to implement periodic updates to the virus scanning software implemented which includes the implementation of updates?

TABLE 23

VITAL RECORD MANAGEMENT: -- Policies and procedures should provide reasonable assurance that appropriate data file and production software backups are maintained off-site.
1. Is off-site disk mirroring being performed? If yes, indicate if this is for every application file, all production servers and system software.
If Yes to question 1: please answer "n/a' to questions 1, 2, 3 and 4. If No to question 1: proceed with question 2 below.
2. Are backups produced daily for every application file and sent to the off-site tape vault?
3. Are full image backups of all production servers produced daily and sent to the off-site tape vault?
4. Is system software backed up periodically and sent to the off-site tape vaults? If Yes, how frequently is this process performed.
5. Is a tape management software package used to track backup tapes that are sent off-site? If Yes, what tape management software package is used.

TABLE 24

WEB SITE -- Policies and procedures should provide reasonable assurance that the Web site is protected from unauthorized access and modification.
1. Are all unnecessary daemons disabled and removed from the system?
2. Are periodic reviews of router and firewall logs performed to validate filter operation?
3. Are all services which are not required (e.g., Telnet) turned off?

4. Is a security software product (e.g. Internet Security Systems' Safesuite) periodically executed to determine potential security vulnerabilities on such interfacing domain components as routers, web servers, mail servers, FTP servers, Name servers, firewalls and network monitors (i.e., tested from inside and outside the firewall)? If Yes, what product(s) is used?
5. If the third party software is branded with the JPMC brand, does the web site include the JPM data privacy statement? If it is branded with the third party provider's brand, do they have a commensurate statement in place?
6. Is there a mechanism in place to capture and record consent of Data Privacy preferences, if necessary by law?
7. Does the privacy statement contain details of cookies or click stream methods used?

[76] As illustrated in Tables. 1-24, the system and process of the present invention provides a systematic, standardized and comprehensive review of the operations of the OSP. For areas that require attention or do not meet policy compliance, a corrective action, risk acknowledgment or risk acceptance process will automatically be invoked. Such processes should identify the condition, remediation plan, identification of accountable personnel and targeted deadlines for implementation.

[77] Returning to Fig. 2, step five (70) of the process requires the user to document the results of her review of the continuity plans and capabilities of the OSP. Continuity relates to the plans and procedures for providing the continuity of business operations in cases of business interruption. Such business interruption can occur due to a variety of reasons including physical facility emergency. The continuity in business operations can be in regard to at least to real estate, and critical business resources such as computers, databases and applications.

[78] Fig. 8 illustrates the user interface screen 550 applicable to the review of the continuity preparedness review of the OSP. Question 575 asks whether or not the OSPs business continuity plan has been tested in the past twelve months. If it has, the user inputs the date the plan was tested. Question 580 prompts the user to indicate when the next test of the continuity plan is scheduled. The questions listed in area 585 require the user to document specific aspects of the OSP's continuity plan. As with the other above described user interface screens, continuity screen 550 provides the user with the ability to answer Yes (555), No (560), N/A (565) to the posed questions. Additionally, screen 550 provides a Comments section 570. In the Comment section 570 the user can enter or attach a description of the control process(es) or any information, that supports or clarifies the user's responses. The user is advised to indicate what evidence exists to support the responses or cross-reference to the supporting documentation.

[79] The most significant of the questions listed in area 585 relate to the existence and adequacy of backup or recovery locations. The purpose of identifying the recovery locations of OSPs is to provide system 10 with the capability, in an emergency situation, to assess whether or not (or when) a particular department can resume operations with its OSP. For example, if the OSP's primary location is in the same geographical location as the department's primary location, in the case of a flood in the zone, it would be reasonable to assume that the OSP will also not be operational.

[80] Furthermore, identification of the OSP's recovery location will enable the organization to assess whether or not OSP is adequately prepared in the case of a disaster. For example, if the OSP has no recovery location, the firm might decide to use another OSP with adequate recovery procedures, or might pressure the existing external OSP to develop such a recovery site.

[81] The structured review provided by system 10 through interface 550 allows business managers and technologists to stage continuity scenarios with OSP relationships and make informed decisions around key processes, people, locations and critical business applications including production, development and QA environments regarding internal and external resources.

[82] The data input through interface 550 introduces enhanced reporting capabilities to track and monitor key issues of the OSP and their ongoing progress to close substantial gaps. Provides real-time, objective data for various scorecards requested enterprise-wide. As further described below, the data with respect to the OSP's continuity preparedness allows system 10 to produce an enterprise-wide "heat map" in the test, plan and execute space including corrective actions plans, risk acknowledgments and board issues of every OSP. System 10 further provides a repository to identify critical incidents and pending resolutions during an event involving an OSP. System 10 further provides the capabilities to link the enterprise's continuity plans to the OSP insuring there is alignment. Finally, system 10 provides a core repository in database 40 (Fig. 1) to manage, monitor and measure key continuity processes regardless of service provider (e.g., internal, external, onshore, offshore).

[83] Step 5 of the process (Fig. 2) is to assist the manager in developing a contact strategy with respect to the OSP for use, for example, during cases of emergency. The contact strategy provides system 10 with complete information regarding each employee that is connected with the OSP relationship, as well as documenting the contacts at the OSP itself.. To this end, separate records are created in system 10 for the identified employees and OSP personnel. Fig.9 illustrates the user interface 600 for accessing the contact records in system 10. The user is able to input new employee or OSP employee contact information through interface 605. The contact records preferably contain: the employee's name; primary work location, primary

work region; primary work branch; primary work phone number; primary work facsimile number; pager number; PIN number for the pager cellular phone number; home phone number; alternate home (e.g., vacation); personal Internet addresses; alternate work location; alternate work address; and alternate work phone number.

[84] The input of all of the employees' personal information allows system 10 to maintains a comprehensive and up to date contact list including key corporate senior executives in addition to all senior LOB business executives. In addition to the above personal information such as phone numbers for office, home, alternate home (e.g., vacation), cellular, personal Internet addresses, pagers, the contact list for key executives includes an identification of the person's alternate/designee.

[85] The final step in the process, step 6 (75 in Fig. 2) is to assess the compliance of the OSP with the privacy policies of the enterprise. Privacy issues with respect to the collection, use and dissemination of personal information are becoming increasingly important for every enterprise to monitor and track. As the laws of each state with respect to the privacy of employees and customers is evolving rapidly, it is very important that the privacy policies of the enterprise are reviewed and updated regularly. As OSPs are increasingly processing data that has a privacy component, it is equally important that the enterprise review the OSP's compliance with the enterprise's privacy policies.

[86] As depicted in Fig. 10, screen area 650 allows the user to select a category of the enterprise's privacy policy for assessing the operations processes and procedures of the OSP. The preferred categories include: Customer Services Processes 655; Data Destruction and Disposal Procedures 660; Data Extraction and Modification 665; Development and QA/UAT Environment Processes 670; Encryption Practices; OSP practices 680; Related Applications and Processes 685; and Website Practices; 690.

Depending on the services being provided by the particular OSP under review, the user may select one or more of categories 655-690.

[87] Screen area 695 depicts the questions posed to the user when she selects the Customer Servicing Processes category 655. As seen in this user interface screen 695, the user is asked to review the training and procedures of the customer service representatives.. For example, the user is asked whether the OSP employee providing customer services has been trained with respect to the safeguarding of private information. Screen 695 is exemplary of the types of questions requiring answers by the user when selecting any of the privacy categories 655-690.

[88] When a user provides a negative answer to any of the questions in any of the assessments in system 10 as described above, system 10 automatically asks the manager if she would like to develop a Corrective Action Plan (CAP) if the gap will be remediated within ninety days. As implied by its name, a Corrective Action Plan is a plan to correct the condition that has caused the manager to answer a question negatively. If the manager answers yes to developing a CAP, system 10 brings the manager to a CAP input screen in which the manager describes the condition which caused the negative response, the reason for the condition (e.g., funding) the plan to correct the condition, the person responsible for seeing that the correction is done, a target date by which the correction will be completed, and any attachments which are required to more fully explain the CAP. The CAP that is developed is stored in the database and appropriately linked to the records for this department.

[89] If the manager says "No" when asked if she wants to develop a CAP, the manager is automatically brought to a Risk Acceptance screen. In this screen, the manager is required to describe the reasons for the requirement of the Risk Acceptance; what compensating controls are in place, if any; the likelihood of an impact due to the risk involved (high, medium or low); a description of the potential

impact; a rating of the potential impact (catastrophic, severe, moderate, negligible); and an implementation plan. The Risk Acceptance by the manager is reviewed and approved by the appropriate LOB management. If the Risk Acceptance is not approved by management, a CAP must be developed in order to correct the risk condition.

[90] One of the significant features of the present invention is the ability of system 10 to rollup all of the collected information into clear and easily comprehensive status report. Figure 11 illustrates one such report, in the form of a computer screen, known as a State of Health Report Card 700. This report 700 provides enhanced capabilities to track and monitor key issues and their ongoing progress to close substantial gaps. Report 700 provides the highest level of status of the reviews of the OSP described above, including corrective actions plans, risk acknowledgments and board issues as further described below. This status screen 700 provides a core repository to manage, monitor and measure all OSPs utilized by the enterprise.

[91] As seen in Figure 11, this status screen contains the status of an OSP 705 corrective actions plans 715, risk acknowledgments 740, and board issues 745. A record 720 is capable of being displayed for each line of business within the organization (only three illustrated in Figure 11). For each record 720, the name of the Senior Business Executive 725 and the name of the Line of Business 730 is displayed. The actual name of the Line of Business 732 is a hyperlink that brings up a status screen comparable to screen 700, except that it shows the status of the elements for the next level down in the corporate hierarchy (e.g., the department level). Using this feature, a user is able to drill down (or roll up) to the level of status desired by the particular user.

[92] The status of a particular element of the OSP review is depicted as a colored icon, e.g., icon 735 Corrective Action Plan 715. Each icon represents a different

status. In addition to each icon being a different color, it is also a different shape. This allows user having devices without color capability to quickly determine the status of a particular item. Figure 12 illustrates a legend containing the different icons and their associated statuses. In the particular statuses depicted in Figure 11, status 735 indicates that there is no Corrective Action Plan in place for the OSPs being employed by this particular line of business. Were there a Corrective Action Plan in place and documented on system 10, by clicking on the status icon 735 in the Corrective Action Plan column 715, the user can immediately bring up the CAP developed by the manager. If the manager did not develop a CAP, but rather performed a Risk Acknowledgement, this is indicated in column 740. Similarly, by clicking on the icon 742 in this column 740, the user will be able to see the specific Risk Acknowledgement developed by the manager.

[93] If the user clicks on one of the status icons in the Outside Service Provider column 705, system 10 drills down the data to the next level of status as illustrated in Fig. 12. State of Health status screen gives the manage a more detailed look at the status of the reviews of any particular OSP that provides services to the particular line of business. Column 805 contains the name of the particular OSP. As seen in Fig. 12, five different OSPs 865 have been identified as performing work for the selected LOB. Column 810 provides the status of the OSP with respect to Managing Risk. Column 815 provides the status of the OSP with respect to the Continuity review. This status is derived by system 10 from the analysis of the results of the review as discussed above in connection with Fig. 8. Column 820 provides the status of the OSP with respect to the Privacy review. This status is derived by system 10 from the analysis of the results of the review as discussed above in connection with Fig. 10. Column 825 provides the status of the OSP with respect to the Financial review. This status is derived by system 10 from the analysis of the results of the review as discussed above in connection with step 3 (60) in Fig. 2. Column 830 provides the

status of the OSP with respect to the Sourcing review. This status is derived by system 10 from the analysis of the results of the review as discussed above in connection with step 3 (60) in Fig. 2. Column 835 provides the status of the OSP with respect to the Legal review. This status is derived by system 10 from the analysis of the results of the review as discussed above in connection with step 3 (60) in Fig. 2. Column 840 provides the status of the OSP with respect to the External Connectivity review. This status is derived by system 10 from the analysis of the results of the review as discussed above in connection with step 3 (60) in Fig. 2.

[94] Column 845 provides the status of the OSP with respect to the Business Impact review. This status is derived by system 10 from the analysis of the results of the review as discussed above in connection with Fig. 4. As previously discussed, the Criticality status determined for the particular OSP is cross-referenced in the OSP description interface as depicted in Fig. 3. Column 850 provides the status of the OSP with respect to the Country Impact review. This status is derived by system 10 from the analysis of the results of the review as discussed above in connection with Fig. 5. Column 855 provides the status of the OSP with respect to any Risk Acknowledgements required by negative assessments of any of the reviews as discussed above. Similarly, column 860 provides the status of the OSP with respect to any Corrective Action Plans required by negative assessments of any of the reviews as discussed above.

[95] Although the present invention has been described in relation to particular embodiments thereof, many other variations and other uses will be apparent to those skilled in the art. It is preferred, therefore, that the present invention be limited not by the specific disclosure herein, but only by the gist and scope of the disclosure.